

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-91295

(P2002-91295A)

(43) 公開日 平成14年3月27日 (2002.3.27)

(51) Int.Cl.⁷

G 0 9 C 1/00

識別記号

6 1 0

F I

G 0 9 C 1/00

テ-マ-ド* (参考)

6 1 0 A 5 J 1 0 4

審査請求 未請求 請求項の数 8 O L (全 13 頁)

(21) 出願番号 特願2001-207327 (P2001-207327)

(22) 出願日 平成13年7月9日 (2001.7.9)

(31) 優先権主張番号 特願2000-212814 (P2000-212814)

(32) 優先日 平成12年7月13日 (2000.7.13)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番1号

(72) 発明者 下山 武司

神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

(72) 発明者 伊藤 孝一

神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

(74) 代理人 100074099

弁理士 大菅 義之 (外1名)

最終頁に続く

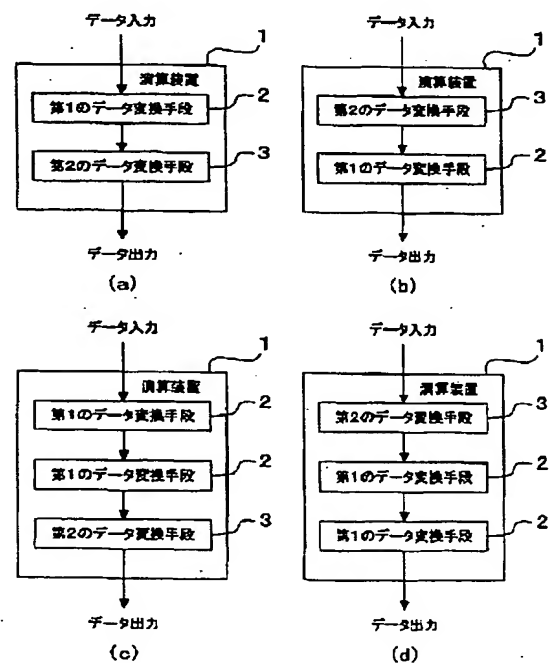
(54) 【発明の名称】 Feistel 構造とSPN構造とを組み合わせた演算装置および演算方法

(57) 【要約】

【課題】 共通鍵ブロック暗号化方式において、演算量を削減させ、かつデータ拡散性能を向上させる。

【解決手段】 Feistel 構造を用いてデータ変換を行う手段2の1つ以上と、SPN構造を用いてデータ変換を行う手段3の1つ以上とを、データ入力とデータ出力との間で縦続的に組み合わせる。またSPN構造内で、固定された半数の入力ビット、および同位置にある半数の出力ビットにのみ関係する線形関係式がすべての入出力データ間で成立する確率が1/2となる非線形変換手段を用いる。

本発明の原理構成ブロック図



【特許請求の範囲】

【請求項1】 データ入力を受け取り、該データ入力に対する演算結果をデータ出力とする演算装置において、Feistel 構造を用いてデータ変換を行う第1のデータ変換手段の1つ以上と、

SPN構造を用いてデータ変換を行う第2のデータ変換手段の1つ以上とを、前記データ入力とデータ出力との間で縦続的に組み合わせられたことを特徴とするFeistel 構造とSPN構造とを組み合わせた演算装置。

【請求項2】 前記SPN構造が、前記データ入力の1ブロックのブロック長をワード長で除算した値の入・出力ビット数を持つ非線形変換手段と、

インタリーブ変換を用いる線形変換手段とを備えることを特徴とする請求項1記載のFeistel 構造とSPN構造とを組み合わせた演算装置。

【請求項3】 前記SPN構造を構成する非線形変換手段として、該非線形変換手段への入力ビットのうちで固定された1つ以上の入力ビットにのみ差分が与えられた入力データの組に対して、前記固定された1つ以上の入力ビットと同じ位置にある固定された1つ以上の出力ビットにのみ出力データの組に差分が現われる確率が0となり、かつ該固定された1つ以上の入力ビット、および該固定された1つ以上の出力ビットにのみ関係する任意の線形関係式がすべての入・出力データ間で成立する確率が $1/2$ となる非線形変換手段を備えることを特徴とする請求項1、または2記載のFeistel 構造とSPN構造とを組み合わせた演算装置。

【請求項4】 データ入力を受け取り、該データ入力に対する演算結果をデータ出力とする演算方法において、Feistel 構造を用いてデータ変換を行う第1のデータ変換ステップの1つ以上と、

SPN構造を用いてデータ変換を行う第2のデータ変換ステップの1つ以上とを、前記データ入力とデータ出力との間で組み合わせて実行することを特徴とするFeistel 構造とSPN構造とを組み合わせた演算方法。

【請求項5】 前記SPN構造を用いる第1のデータ変換ステップにおいて、前記データ入力の1ブロックのブロック長をワード長で除算した値を入・出力ビット数とする非線形変換と、インタリーブ変換を用いる線形変換とを実行することを特徴とする請求項4記載のFeistel 構造とSPN構造とを組み合わせた演算方法。

【請求項6】 前記SPN構造内で実行されるべき非線形変換として、該非線形変換においての入力ビット数のうちで固定された1つ以上の入力ビットにのみ差分が与えられた入力データの組に対して、前記固定された1つ以上の入力ビットと同じ位置にある固定された1つ以上の出力ビットに

のみ出力データの組に差分が現われる確率が0となり、かつ該固定された1つ以上の入力ビット、および該固定された1つ以上の出力ビットにのみ関係する任意の線形関係式がすべての入・出力データ間で成立する確率が $1/2$ となる非線形変換を実行することを特徴とする請求項4、または5記載のFeistel 構造とSPN構造とを組み合わせた演算方法。

【請求項7】 データ入力を受け取り、該入力データに対する演算結果をデータ出力とする演算を実行する計算機によって使用される記憶媒体において、Feistel 構造を用いてデータ変換を行う第1のデータ変換ステップの1つ以上と、

SPN構造を用いてデータ変換を行う第2のデータ変換ステップの1つ以上とを、前記データ入力とデータ出力との間で組み合わせて実行させる機能を備えるプログラムを格納した計算機読出し可能可搬型記憶媒体。

【請求項8】 データ入力を受け取り、該入力データに対する演算結果をデータ出力とする演算を実行する計算機によって使用されるプログラムにおいて、Feistel 構造を用いてデータ変換を行う第1のデータ変換手順の1つ以上と、

SPN構造を用いてデータ変換を行う第2のデータ変換手順の1つ以上とを、前記データ入力とデータ出力との間で組み合わせて実行させる機能を備えるプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は共通鍵ブロック暗号方式に係り、更に詳しくはFeistel 構造とSPN構造とを組み合わせ、かつSPN構造に特別の工夫を行ってデータの拡散性を向上させる暗号化装置、および暗号化方法に関する。

【0002】

【従来の技術】 高度情報化社会を迎え、情報セキュリティの確保は緊急の課題となっている。情報セキュリティの基本となるのはデータの暗号化である。高度情報化社会において高速、かつ安全な通信を実現するために共通鍵ブロック暗号は不可欠の技術である。この共通鍵ブロック暗号のアルゴリズムとして従来様々な方式が提案されているが、それらは基本的にはFeistel 構造と呼ばれる構造の繰返しか、あるいはSPN構造と呼ばれる構造の繰返しのいずれかであった。

【0003】 図12はFeistel 構造の説明図である。同図において、例えば入力128ビットは右側64ビットと左側64ビットに分割され、右側64ビットはF関数51と呼ばれる非線形関数に入力され、その出力と左側64ビットとがXOR52によって排他的論理和がとられ、その結果が出力128ビットのうちの右側64ビットとして出力され、左側64ビットとしては入力128ビットのうちの右側64ビットがそのまま出力される。このようなFeistel 構造が、例えば16段繰返され

て、暗号化が行われる。

【0004】図13はSPN構造の例である。この構造においては、Sボックスと呼ばれる非線形変換53と、線形変換P54とが組み合わされて用いられる。SボックスのSはサブステティューション、すなわち換字を、関数Pはパーミュテーション、すなわち置換を意味するが、現在ではSはより一般的に非線形写像を、またPは置換だけではなく、ビット単位の線形変換を指すものとなっている。

【0005】いずれにせよ、このようなSPネットワーク（SPN）構造が多段に繰り返されることによって暗号化が行われる。なお図12のFeistel 構造内のF関数として後述するようにSPN構造が用いられるが、図12は全体としてはFeistel 構造を示すものである。

【0006】

【発明が解決しようとする課題】以上のような共通鍵ブロック暗号方式においては、Feistel 構造、SPN構造のいずれを用いるとしても、なるべく少ない段数でデータの安全性が保証されるような暗号化を行う必要がある。しかしながら、まずFeistel 構造を用いる場合には1段で入力データ長の半分しか攪拌されず、ワード内のデータ攪拌には効果があるが、ワードを越えたデータ攪拌能力が劣るという問題点がある。また入出力が対称の形式となっていることから、暗号としては繰返し型の差分近似式、または線形近似式が存在する可能性があり、差分攻撃や線形攻撃にさらされる危険性があるという問題点があった。

【0007】これに対してSPN構造を用いる場合には、ワード間のデータ攪拌性には効果があり、入出力が非対称の形式であるという長所を持つが、入力データ長全体を分割して複数のSボックスに入力させる必要があり、Sボックスは一般にメモリ内にテーブルとして保持されるものを使用するため、Sボックスの数が増えることによってテーブル参照回数が増加し、SPN構造だけを何段も組み合わせる場合には、処理に時間がかかるという問題点があった。

【0008】本発明の課題は、上述の問題点に鑑み、Feistel 構造とSPN構造とを組み合わせることでそれぞれの欠点をできるだけ解消させる暗号化を行うと共に、SPN構造内のSボックスにおいてもデータ攪拌効果を更に向上させることによって、演算量をできるだけ削減し、かつデータ拡散性能に優れた暗号化装置、および暗号化方法を提供することである。

【0009】

【課題を解決するための手段】図1は本発明の演算装置の原理構成ブロック図である。同図はデータ入力を受け取り、そのデータ入力に対する演算結果をデータ出力とする演算装置を示す。この演算装置1では、Feistel 構造を用いてデータ変換を行う第1のデータ変換手段2の1つ以上と、SPN構造を用いてデータ変換を行う第2

のデータ変換手段3の1つ以上とが、データ入力とデータ出力との間で縦続的に組み合わせられる。

【0010】図1（a）においては、データ入力に対して最初に第1データ変換手段2、次に第2のデータ変換手段3が用いられ、（b）においては逆に最初に第2のデータ変換手段3が、次に第1のデータ変換手段2が用いられる。

【0011】（c）においては先ず第1のデータ変換手段2が2段用いられた後に、第2のデータ変換手段3が用いられる。（d）においては逆に第2のデータ変換手段3が用いられた後に、第1のデータ変換手段2が2段連続に用いられてデータ出力が行われる。

【0012】このように本発明においては第1のデータ変換手段2の1つ以上と、第2のデータ変換手段3の1つ以上とが組み合わせられて用いられるが、Feistel 構造を用いる第1のデータ変換手段2については、1段ではデータの片側しか攪拌されないため、例えば2段連続的に用いられてデータの両側の攪拌が行われるような形式で組み合わせが行われる。なお、2つのデータ変換手段をさらに多数組み合わせることも当然可能である。

【0013】本発明の実施の形態においては、SPN構造の中にデータ入力の1ブロックのブロック長、例えば128ビットをワード長32ビットで割算した値、例えば4ビットの入・出力ビット数を持つ非線形変換手段、例えばSボックスと、インタリーブ変換を用いる線形変換手段とを備えることもできる。

【0014】また発明の実施の形態においてはSPN構造を構成する非線形変換手段、例えばSボックスとして入力ビット数、例えば4ビットのうちで、1つ以上、例えば右側2ビットにのみ差分が与えられた入力データの組に対して、同じ位置、すなわち右側2ビットにのみ出力データの組に差分が現われる確率が0となり、かつ例えば右側2ビットの入力ビットおよび右側2ビットの出力ビットにのみ関係する任意の線形関係式がすべての入出力データ間で成立する確率が $1/2$ となる非線形変換手段を備えることもできる。

【0015】本発明の演算方法においては、データ入力に対する演算結果をデータ出力とする演算方法において、Feistel 構造を用いてデータ変換を行う第1のデータ変換ステップの1つ以上と、SPN構造を用いてデータ変換を行う第2のデータ変換ステップの1つ以上とを、データ入力とデータ出力の間で組み合わせる実行する演算方法が用いられる。

【0016】発明の実施の形態においては、この演算方法内のSPN構造を用いた第1のデータ変換ステップにおいて、データ入力の1ブロックのブロック長をワード長で割った値を入出力ビット数とする非線形変換と、インタリーブ変換を用いる線形変換とを実行することもできる。

【0017】また本発明の実施の形態においては、この

SPN構造内で実行されるべき非線形変換として、入力ビット数のうちで1つ以上、例えば右側半数の入力ビットにのみ差分が与えられた入力データの組に対して、同じ右側半数の出力ビットにのみ出力データの組に差分が現われる確率が0となり、かつ右側半数の入力ビット、および右側半数の出力ビットにのみ関係する任意の線形関係式がすべての入・出力データの間で成立する確率が $1/2$ となる非線形変換を実行することもできる。

【0018】更に本発明においては、データ入力を受け取り、そのデータ入力に対する演算結果をデータ出力とする演算を実行する計算機によって使用される記憶媒体として、Feistel 構造を用いてデータ変換を行う第1のデータ変換ステップの1つ以上と、SPN構造を用いてデータ変換を行う第2のデータ変換ステップの1つ以上とを、データ入力とデータ出力との間で組み合わせて実行させる機能を有するプログラムを格納した計算機読出し可能可搬型記憶媒体が用いられる。

【0019】更にまた本発明においては、データ入力を受け取り、そのデータ入力に対する演算結果をデータ出力とする演算を実行する計算機によって使用されるプログラムとして、Feistel 構造を用いてデータ変換を行う第1のデータ変換手順の1つ以上と、SPN構造を用いてデータ変換を行う第2のデータ変換手順の1つ以上とを、データ入力とデータ出力との間で組み合わせて実行させる機能を有するプログラムが用いられる。

【0020】以上のように本発明によれば、Feistel 構造とSPN構造とがデータ入力とデータ出力との間で組み合わせられて演算が実行され、更にSPN構造の内部で、例えば右側半数の入力ビットにのみ差分が入力データの組に現われた場合、右側半数の出力ビットには出力データの組に差分が現われないような非線形変換が用いられる。

【0021】

【発明の実施の形態】本発明においては、Feistel 構造とSPN構造とが組み合わされて、演算装置、または演算方法が構成されるが、そのような演算装置および演算方法として、入力された平文を暗号化して出力する暗号文生成装置、および生成方法を発明の実施形態として説明する。

【0022】図2はそのような暗号文生成装置のシステム構成ブロック図である。同図において、暗号文生成装置は処理装置10、入力ファイル11、出力ファイル12、表示装置13、および入出力装置14によって構成されている。

【0023】処理装置10の内部には、使用されるFeistel 構造を決定するFeistel 構造決定部16、SPN構造を決定するSPN構造決定部17、Feistel 構造とSPN構造とを組み合わせた暗号化アルゴリズムを決定する暗号化アルゴリズム決定部18、その暗号化アルゴリズムに従って平文を暗号化する暗号文生成部19を備え

ている。

【0024】入力ファイル11には暗号化されるべき入力データとしての平文、入力データ1ブロックのビット長 n 、処理装置10による演算に適当なワードのビット長 w 、および後述するようにSPN構造の中で用いられる線形変換としてのインタリーブ変換の内容などが格納されている。

【0025】また出力ファイル12には、Feistel 構造決定部16によって決定されるFeistel 構造に用いられるF関数、SPN構造決定部17によって決定されるSボックスの非線形関数に相当する写像 S 、および暗号化アドレス決定部18によって決定されたFeistel 構造とSPN構造の組合せとしての暗号化アルゴリズムなどが格納される。

【0026】図3は本実施形態におけるFeistel 構造とSPN構造との組合せ、すなわち暗号化アルゴリズム決定部18によって決定された暗号化アルゴリズムの例である。同図において、入力データに対してまずFeistel 構造20a、20bによる演算が2段行われる。その後SPN構造23による演算が行われ、その結果に対して更に2段のFeistel 構造20c、20dによる演算が行われ、その結果が暗号文として出力されることになる。

【0027】図3においては、1段のFeistel 構造によっては入力データのうち片側半分しか攪拌されないため、Feistel 構造が2段重ねて用いられると共に、後述するようにSPN構造23にワード内の攪拌効果を大きくする工夫が取り入れられる。すなわちSボックスで用いられる非線形関数に対して、後述する図8、図9のような性質を持つ関数を用いてワード内の攪拌効果を大きくすると共に、更に線形変換としてインタリーブ変換を用いることによって、1つのブロックを構成する複数のワードの間での攪拌効果が大きくなるようにSPN構造が構成される。

【0028】なお、Feistel 構造を3段以上連続して用いるとSPN構造を組み合わせた効果が薄れてくるため、図3ではSPN構造が2段のFeistel 構造の間に挿入された組合せとなっている。

【0029】図4はそのSPN構造23の概略の説明図である。同図において入力データ、例えば128ビットに対してまずインタリーブ変換24が行われ、例えば32ビットで構成される4つのワード間のデータの攪拌が行われる。その攪拌結果は複数のSボックス25に与えられ、Sボックス25の出力に対してインタリーブ逆変換26が行われて、SPN構造の出力となる。

【0030】図5は本実施形態における暗号文生成処理の全体フローチャートである。同図において処理が開始されると、まずステップS1で平文、すなわち入力データブロックのビット長 n が入力されて、ステップS2でFeistel 構造 R が定められる。本実施形態においては、このFeistel 構造内の非線形関数 F として任意の関数を

用いることができるものとするが、その例については図6で説明する。

【0031】続いてステップS3で演算器に適するワードのビット長 w が入力され、ステップS4でSPN構造Bが定められる。このSPN構造Bについては、図4で説明したようにインタリーブ変換とSボックスの非線形関数の内容が問題となるが、これらについては後述する。

【0032】そしてステップS5で、1段以上のFeistel 1 構造と1段以上のSPN構造とが組み合わせられて、例えば図3で示したような暗号化アルゴリズムが定められ、ステップS6でその暗号化アルゴリズムに従って入力データとしての平文が暗号化されて暗号文が生成され、処理を終了する。

【0033】図6は本実施形態においてFeistel 構造の内部で用いられるF関数の例である。このF関数としては、前述のように任意の非線形関数を用いることができ、その意味でF関数として図6のものをを用いなければならない理由はないが、その構成について特徴的な部分を中心に説明する。

【0034】図6において、入力データ64ビットはそれぞれ右側、左側32ビットずつに分割され、XOR30a、30bによってkey1とkey2との排他的論理和がそれぞれとられ、6ビットまたは5ビットずつに分割されて、それぞれ6つのSボックス31に入力される。一般的にはSボックスとして全てのSボックスの入出力ビット数が等しいものを並べて使う場合が多い。ここでは6ビット入出力のSボックスと5ビットの入出力のSボックスとを混在させて用いているが、その詳細については説明を省略する。

【0035】それぞれ6個のSボックス31の出力はMDS変換部32a、32bに与えられる。ここでMDS変換部は、図12で説明したSPN構造における関数Pに相当し、その意味ではFeistel 構造内のF関数はSPN構造を持つともいえるが、このP関数におけるデータの拡散性を定義する1つの概念としての分岐数を最大とする線形変換層がMDS変換部である。この分岐数は、暗号に対する差分攻撃や、線形攻撃に対する強度を評価するパラメータであり、その詳細については次の文献で説明されている。

文献) 共通鍵ブロック暗号の選択/設計/評価に関するドキュメント、通信・放送機構

MDS変換部32a、32bの出力は、それぞれXOR33a、33bに与えられ、排他的論理和がとられるが、例えばMDS変換部32aの出力32ビットに対しては、0x5555 5555との論理積がとられた後にExオア33bに与えられる。このような論理積がとられるのは、MDS変換部32a、32bの出力がそのまま与えられるのでは、Exオア33a、33bの出力は同じになってしまうためである。ここでMDS変換部

32aの出力と論理積がとられるデータは2進数では010101・・・0101(32ビット)であり、またMDS変換部32bの出力と論理積がとられるデータは101010・・・1010(32ビット)である。

【0036】図7は図5のステップS4、すなわちSPN構造Bの決定処理の詳細フローチャートである。同図において処理が開始されると、まずステップS9で入出力ビット数が求められた後に、ステップS10でランダムな写像Sが新しく選択される。この写像Sは、図5のステップS1で入力されたブロックのビット長 n を、ステップS3で入力されたワードのビット長 w で割った結果としての、 r ビット入出力の1対1写像である。

【0037】例えば平文、すなわち入力データのブロックのビット長 n が128ビットであり、ワード長 w が32ビットであるとする、 r は4ビットとなり、4ビット入出力のランダムな写像Sが選択される。

【0038】図7のステップS11で、写像Sを対象として固定された半数の入力ビット、例えば4ビットのうち2ビットにのみ差分が与えられた入力データの組に対して、同じ位置にある固定された半数の出力ビットにのみ出力データの組に差分が現われる確率が0であるか否かが判定され、0でない場合にはステップS10に戻り、新しいランダムな写像Sの選択以降の処理が繰り返される。

【0039】ステップS11で確率が0と判定されると、ステップS12で写像Sを対象として固定された半数の入力ビット、および例えば同じ位置にある固定された半数の出力ビットのみに関係する任意の線形関係式について、全ての入出力ビットデータ間でその線形関係式が成立する確率が $1/2$ であるか否かが判定され、 $1/2$ でない場合にはステップS10以降の処理が繰り返される。なおステップS11、S12における判定については図8、図9を用いて更に後述する。

【0040】ステップS12で確率が $1/2$ である場合には、ステップS13でその写像Sとインタリーブ変換、例えば図10で後述するインタリーブ変換であって、図2の入力ファイル11に格納されているインタリーブ変換とが組み合わせられてSPN構造Bが定められ、処理を終了する。

【0041】図8は図7のステップS11で判定される確率の例である。この例は、4ビットを入出力ビット数とする非線形のS関数として

S: (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15) \rightarrow (1, 9, 6, 12, 7, 2, 15, 11, 14, 0, 5, 10, 4, 3, 8, 13)

の関数を用いた場合の例であり、入力差分に対して出力差分が現われる確率としての $x/16$ の x を表わしたものである。なおこの非線形S関数の入出力関係において、例えば最後の10進15に対して10進13が出力されること、すなわち2進数1111に対して1101が出

力されることが示されている。

【0042】図8において4ビットのうち右側半分に入力差分が表われている上の3行においては、対応する位置の片側半分に出力差分が現われる確率、すなわち左側3列の確率は0であることが、また左側半分に入力差分が現われている入力データの組、すなわち下側3行に対しては左側半分に入力差分が現われる確率、すなわち右側3列の確率が0であることが示されている。

【0043】図8において、例えば入力差分が(0001)であり、かつ出力差分が(0100)である入出力データ組は入力組(0110)、(0111)に対する出力組(1111)、(1011)と、入力組(0111)、(0110)に対する出力組(1011)、(1111)の2組だけであることが計算によって確認されている。

【0044】図9は図7のステップS12で判定される確率の例を示す。この確率は前述の非線形S関数に対する確率を示すものである。すなわち、片側2入力ビットおよび片側2出力ビットのみに関係した任意の全ての線形関係式について、全入出力ビットデータ間でその線形関係式が成立する確率 $(8-x)/16$ を決める x を示すものである。

【0045】図9において、右側2入力ビットと右側2出力ビットとにそれぞれ差分が現われるのは上3行の左側3列であり、このような入出力ビットデータ間で線形関係式が成立する確率を示す x の値が0であることから、その確率は $8/16$ 、すなわち $1/2$ となる。

【0046】同様に左側2入力ビット、左側2出力ビットに差分が現われるのは、下3行のうち右側3列であり、これらの入出力データ間においても線形関係式の成立確率は $1/2$ となる。線形関係式の成立確率が $1/2$ となるということは、その入出力データ間でその線形関係式が成立することもあり、また成立しないこともあることを示し、その線形関係式自体に意味がないことを示している。

【0047】入出力ビットに関するある線形式の値が常に0、または1となると、入出力の間にその線形式が成立することになる。暗号においては入出力が線形関係からできるだけ離れていることが望ましく、その意味で前述の成立確率 $1/2$ という状況が望ましい。

【0048】入力を (x_0, x_1, x_2, x_3) 、出力を (y_0, y_1, y_2, y_3) とし、入力(0001)、出力(0100)に関係する線形式 $x_3 + y_1$ の値を調べることとする。前述の写像Sで入力 $1 = (0001)$ に対する出力は $9 = (1001)$ であることから、 $x_3 + y_1 = 1 + 0 = 1$ となる。同様にして、すべての入出力の間で $x_3 + y_1$ の値は次のように求められる。

【0049】

In 0, Out 1 → 0

In 1, Out 9 → 1

In 2, Out 6 → 1

In 3, Out c → 0

In 4, Out 7 → 1

In 5, Out 2 → 1

In 6, Out f → 1

In 7, Out b → 1

In 8, Out e → 1

In 9, Out 0 → 1

In a, Out 5 → 1

In b, Out a → 1

In c, Out 4 → 1

In d, Out 3 → 1

In e, Out 8 → 0

In f, Out d → 0

この計算によって、 $x_3 + y_1 = 1$ という線形式が成立する入出力関係は12となり、確率が $12/16$ となることから図9内で対応する x の値は-4となる。

【0050】図10は図4で説明したインタリーブ変換の例である。同図において、例えばSPN構造への入力データは、A、B、C、Dの4つの部分に分割され、分割されたデータは4行で示されるような形式に変換される。更にA、B、C、Dのデータが列に並ぶように変換され、最終的にA、B、C、Dのデータのうちの最初の部分が1番目に並べられ、次の部分が2番目に、以下同様に並べられるような形式に変換されて、例えばA、B、C、Dの最初の部分、すなわち1番目に並べられたデータが、図4で最も左側にあるSボックス25に入力されることになる。

【0051】例えばAを32ビット変数X、BをY、CをZ、DをW（それぞれ32ビット変数）に割り当て、 $X = (x_0, x_1, \dots, x_{31})$ 、 $Y = (y_0, y_1, \dots, y_{31})$ 、 $Z = (z_0, z_1, \dots, z_{31})$ 、 $W = (w_0, w_1, \dots, w_{31})$ とすると、図10のインタリーブ変換の出力は $(x_0, y_0, z_0, w_0, x_1, y_1, z_1, w_1, \dots, x_{31}, y_{31}, z_{31}, w_{31})$ となる。

【0052】このように本実施形態においては、非線形S関数と、線形変換としてのインタリーブ変換とを組み合わせることによって、入力データの攪拌性能の向上が図られる。

【0053】図8、図9で説明したように、Sボックスの入力の片側2ビット、例えば右側2ビットに入力差分が与えられた時、右側2ビットに出力差分が現われる確率は0であり、左側2ビットに出力差分が現われる確率が0とならないことから、右側半分に入力差分が与えられた入力データの組に対しては左側にその影響が現われることになり、データの攪拌効果が得られる。

【0054】図9では右側2ビットの入力ビットと出力ビットのみに関係する線形関係式の成立確率が $1/2$ と

なる。すなわちその線形関係式に意味がないのに対して、右側2ビットと左側2ビットのみに関係した線形関係式については、その成立確率が $1/2$ より大きくなるものが明らかに存在することになる。右側2ビットと左側2ビットとを関係づける線形関係式によってデータの攪拌効果が得られることになる。

【0055】図11は本実施形態におけるプログラムのコンピュータへのローディングの説明図である。本発明の実施形態としての暗号化装置、例えば図2に示したシステムなどは、当然一般的なコンピュータシステムによって構成することができる。図11はそのようなシステムの構成を示し、コンピュータ41は本体42とメモリ43とによって構成されている。メモリ43はランダムアクセスメモリ(RAM)、ハードディスク、磁気ディスクなどの記憶装置であり、本発明の特許請求の範囲第7項のプログラムや、図5、図7で説明したプログラムなどはメモリ43に格納され、そのプログラムが本体42によって実行されることによって、本発明の演算方法が実現され、入力データに対する暗号化が行われる。

【0056】本発明を実現するためのプログラムは、プログラム提供者側からネットワーク44を介してコンピュータ41にロードされることも、また市販され、流通している可搬型記憶媒体45に格納され、そのプログラムがコンピュータ41にロードされることによって実現されることも可能である。可搬型記憶媒体45としてはフロッピーディスク、CD-ROM、光ディスク、光磁気ディスクなど様々な形式の記憶媒体を使用することができ、前述のプログラムなどがこのような記憶媒体に格納され、コンピュータ41にロードされることによって、本実施形態における暗号化アルゴリズムが出力され、その暗号化アルゴリズムを用いて入力データに対する暗号文を生成することが可能となる。

【0057】

【発明の効果】以上詳細に説明したように、本発明によればワード内でのデータの攪拌、および拡散性能に優れたFeistel構造と、ワード間の攪拌性や、高速演算性、入出力についての非対称性などの性質を持つSPN構造とを組み合わせることによって、暗号化演算の高速性を

図ると共に、暗号の安全性を向上させることができる。更にSPN構造におけるSブロックの非線形関数として、データの攪拌がデータの片側に偏らないような写像を用いることによりデータ攪拌性を向上させると共に、インタリーブ変換を用いることによってワード間のデータの攪拌性を更に向上させることができ、共通鍵ブロック暗号の性能向上に寄与するところが大きい。

【図面の簡単な説明】

【図1】本発明の原理構成ブロック図である。

【図2】本発明における暗号化装置のシステム構成ブロック図である。

【図3】Feistel構造とSPN構造の組合せの例を示す図である。

【図4】SPN構造の構成例を示す図である。

【図5】暗号化アルゴリズムの決定と入力データの暗号化処理の全体処理フローチャートである。

【図6】Feistel構造で用いられるF関数の例を示す図である。

【図7】SPN構造決定処理の詳細フローチャートである。

【図8】S関数に与えられる入力差分に対して出力差分が現われる確率を説明する図である。

【図9】S関数における入出力ビットの間の線形関係式の成立確率を説明する図である。

【図10】インタリーブ変換の例を説明する図である。

【図11】プログラムのコンピュータへのローディングを説明する図である。

【図12】Feistel構造の例を示す図である。

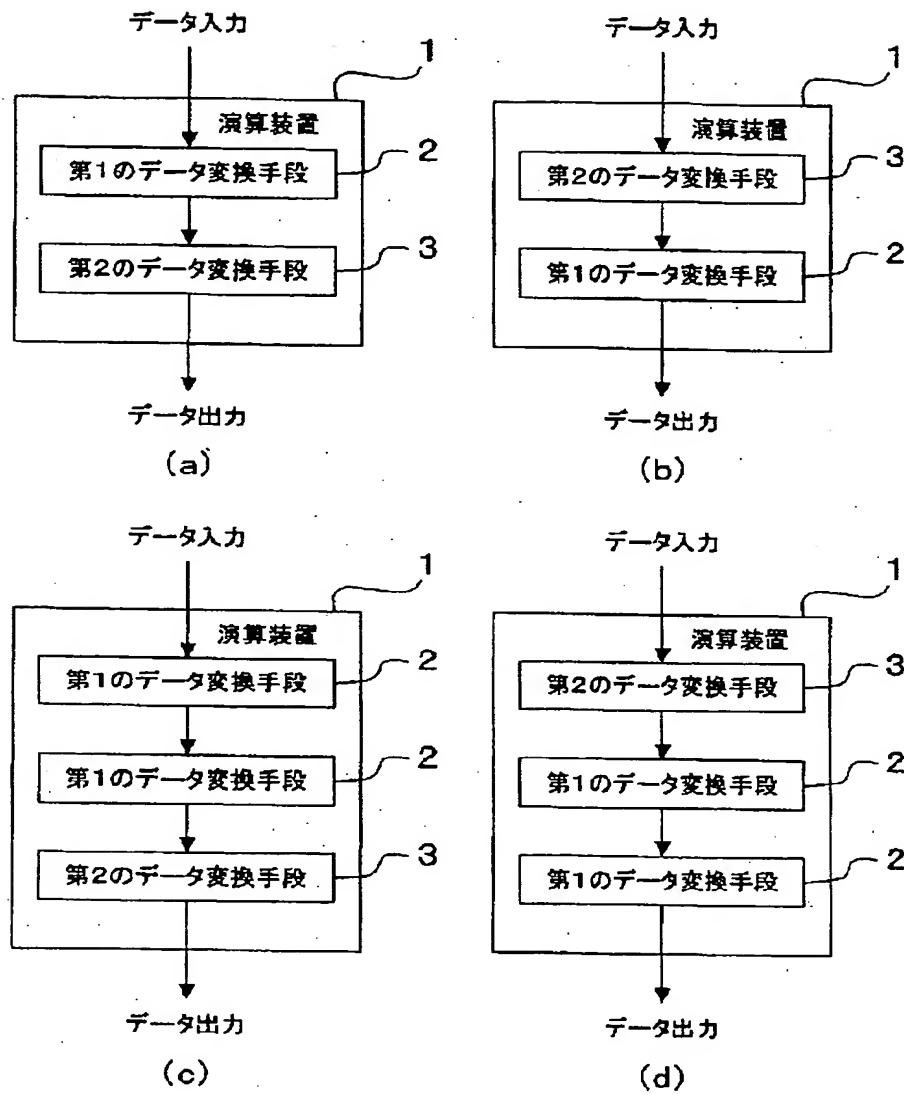
【図13】SPN構造の例を示す図である。

【符号の説明】

- 1 演算装置
- 2 第1のデータ変換手段
- 3 第2のデータ変換手段
- 10 処理装置
- 11 入力ファイル
- 12 出力ファイル
- 13 表示装置

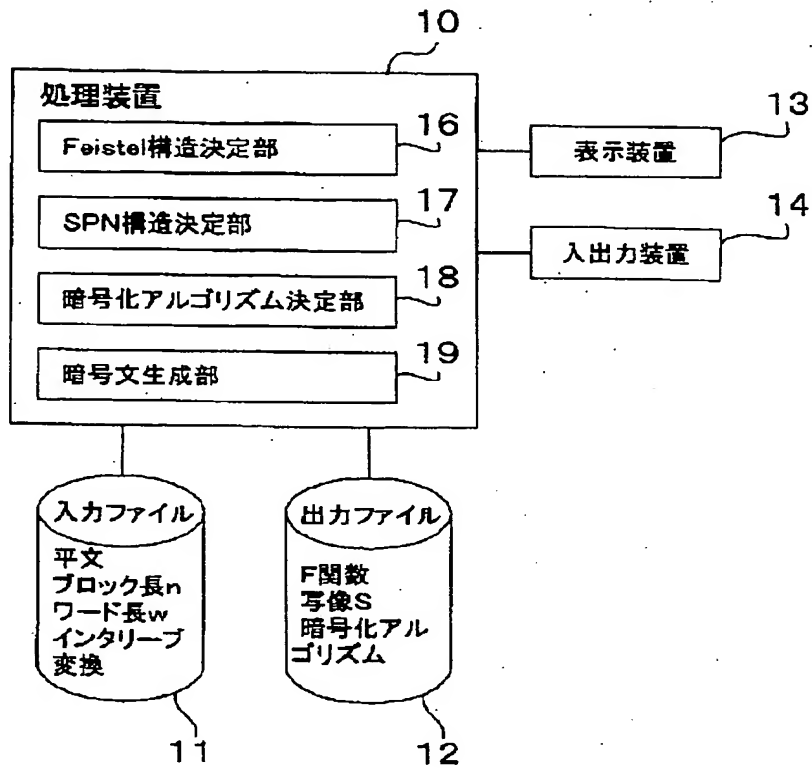
【図1】

本発明の原理構成ブロック図



【図2】

本発明における暗号化装置のシステム構成ブロック図



【図8】

S関数に与えられる入力差分に対して
出力差分が現われる確率を説明する図

入力差分	出力差分					
	(0001)	(0010)	(0011)	(0100)	(1000)	(1100)
(0001)	0	0	0	2	2	0
(0010)	0	0	0	0	2	2
(0011)	0	0	0	2	0	2
(0100)	0	0	2	0	0	0
(1000)	2	0	4	0	0	0
(1100)	4	2	0	0	0	0

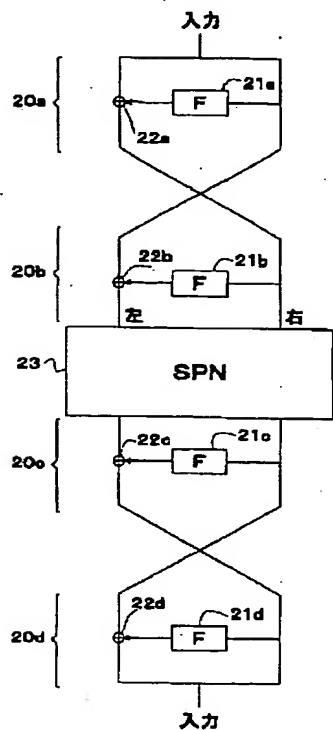
【図9】

S関数における入出力ビットの間の
線形関数式の成立確率を説明する図

入力ビット	出力ビット					
	(0001)	(0010)	(0011)	(0100)	(1000)	(1100)
(0001)	0	0	0	-4	2	-2
(0010)	0	0	0	2	4	2
(0011)	0	0	0	-2	-2	0
(0100)	2	2	-4	0	0	0
(1000)	-2	-2	0	0	0	0
(1100)	0	4	0	0	0	0

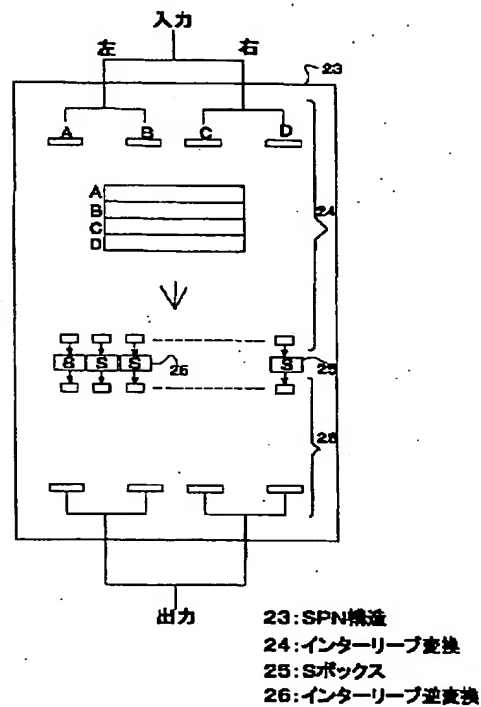
【図3】

Feistel構造とSPN構造の組合わせの例を示す図



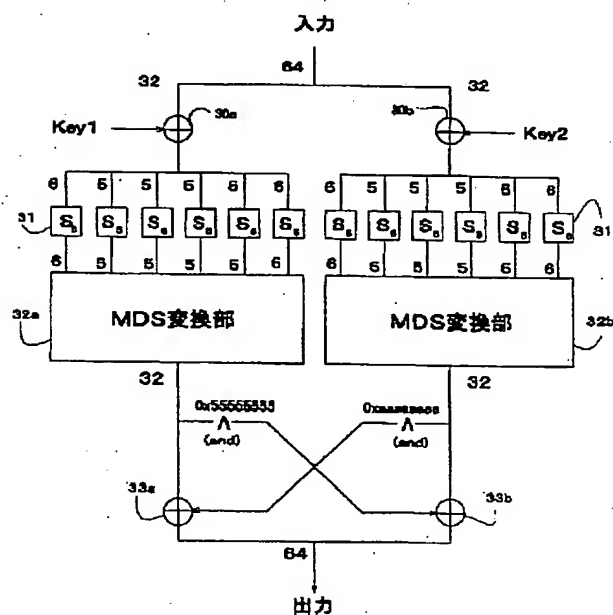
【図4】

SPN構造の構成例を示す図



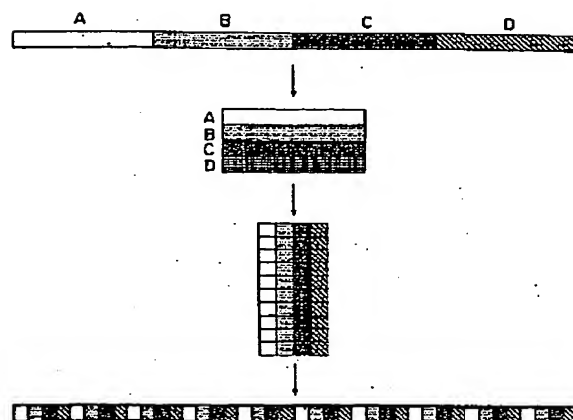
【図6】

Feistel構造で用いられるF関数の例を示す図



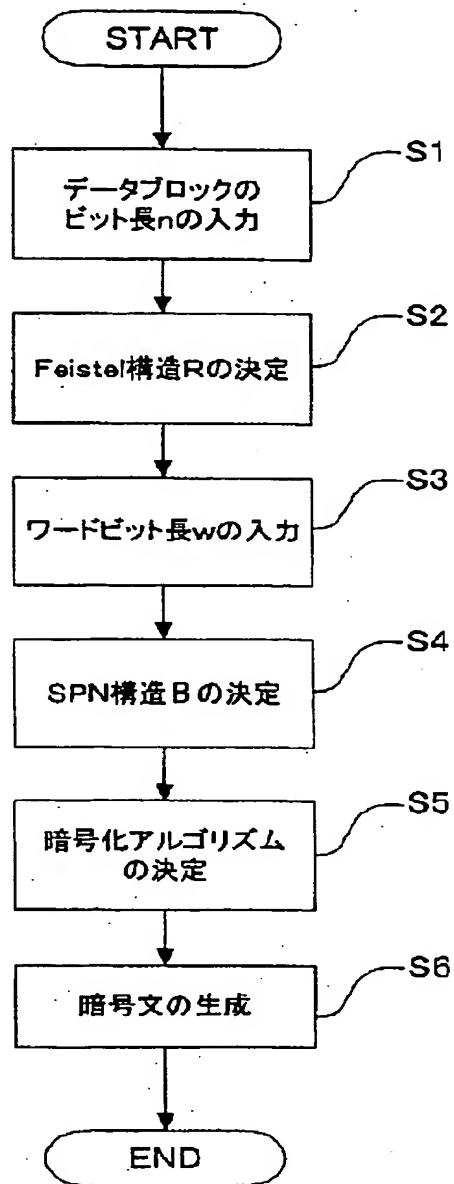
【図10】

インターリーブ変換の例を説明する図



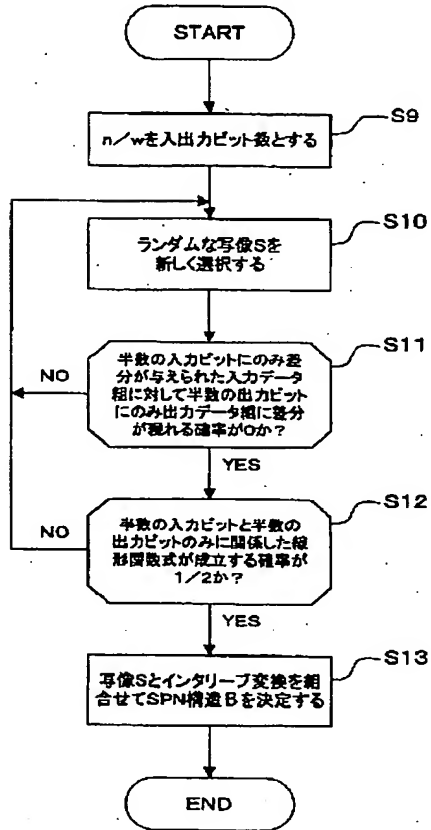
【図5】

暗号化アルゴリズムの決定と
入力データの暗号化処理の全体処理フローチャート



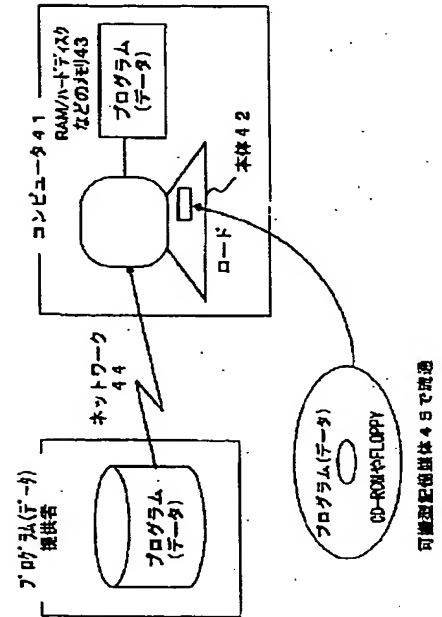
【図7】

SPN構造決定処理の詳細フローチャート



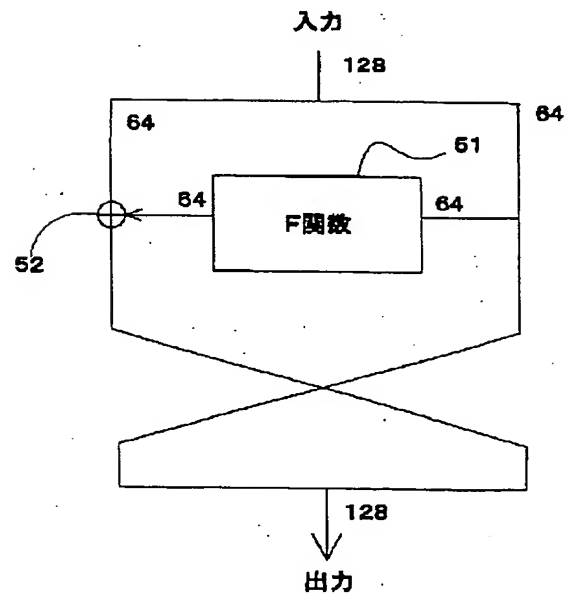
【図11】

プログラムのコンピュータへのローディングを説明する図



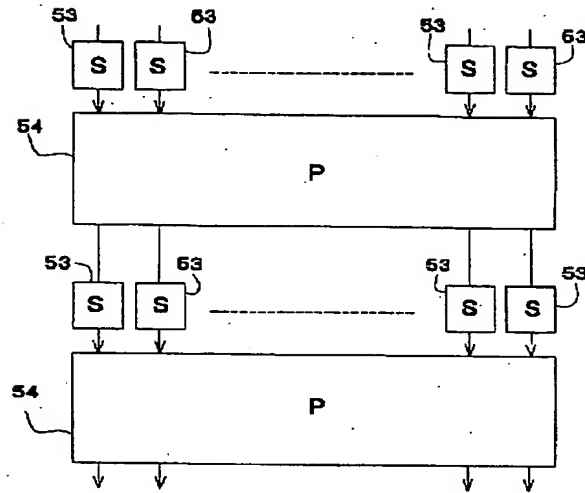
【図12】

Feistel構造の例を示す図



【図13】

SPN構造の例を示す図



S:非線形変換、P:線形変換

フロントページの続き

(72)発明者 武仲 正彦
 神奈川県川崎市中原区上小田中4丁目1番
 1号 富士通株式会社内
 (72)発明者 鳥居 直哉
 神奈川県川崎市中原区上小田中4丁目1番
 1号 富士通株式会社内

(72)発明者 矢嶋 純
 神奈川県川崎市中原区上小田中4丁目1番
 1号 富士通株式会社内
 (72)発明者 屋並 仁史
 神奈川県川崎市中原区上小田中4丁目1番
 1号 富士通株式会社内
 (72)発明者 横山 和弘
 神奈川県川崎市中原区上小田中4丁目1番
 1号 富士通株式会社内

Fターム(参考) 5J104 AA01 AA18 JA12 NA20